

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants: Moskowitz et al.

Art Unit: 3639

Serial Number: 09/990,842

Examiner: Nelson, Freda

Filing Date: 11/21/2001

Confirmation No.: 2704

Title: SECURE METHOD AND SYSTEM
FOR DETERMINING CHARGES
AND ASSURING PRIVACY

Docket No.: CHA920010021US1
(IBMC-0038)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS

This is an appeal from the Final Rejection (OA) dated April 7, 2008, rejecting claims 1-6, 8-17, 19-25 and 33-38. The requisite fee set forth in 37 C.F.R. §1.17 (c) has been submitted on June 9, 2008.

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case includes claims 1-38. Claims 1-6, 8-17 and 19-38 remain pending, among which claims 1-6, 8-17, 19-25 and 33-38 stand rejected, and form the basis of this appeal, and claims 26-32 are withdrawn from consideration; claims 7 and 18 are cancelled. No claim has been allowed. The rejections of claims 1-6, 8-17, 19-25 and 33-38 are being appealed.

STATUS OF AMENDMENTS

No amendment has been filed following the Final Rejection of April 7, 2008.

SUMMARY OF THE CLAIMED SUBJECT MATTER

A first aspect of the present invention (e.g., claim 1) provides a system (see, e.g., Figure 1, remote apparatus 10 + central server 12) for processing usage data within a local data processing system (11) installed on a remote apparatus (10), wherein the local data processing system (11) comprises: a sensor (monitoring system 14) for gathering usage data from the remote apparatus (10) (page 6, lines 6-7); and a processor (16) for processing the gathered usage data and calculating a charge based on the gathered usage data (page 6, lines 10-11); and a security system (18) including an encryption system for encrypting usage data transmitted between the sensor and the processor (page 6, lines 12-14 and page 11, lines 3-9).

A second aspect of the present invention (e.g., claim 16) provides a system (see, e.g., Figure 1, remote apparatus 10 + central server 12) for managing usage data collected on a remote apparatus (10), comprising: a local data processing system (11) having: a

monitoring system (14) for gathering usage data from the remote apparatus (page 6, lines 6-7); a processor (16) for processing the usage data (page 6, lines 10-11); a communications system (20) for communicating the processed usage data (page 6, lines 15-16); and a security system (18) for securing the usage data, wherein the security system includes an encryption system for encrypting usage data communicated from the monitoring system to the processor (page 6, lines 12-14 and page 11, lines 3-9).

A third aspect of the present invention (e.g., claim 23) provides a system (remote apparatus 10 + central server 12) for managing usage information collected on a remote apparatus (10), comprising: a central server (12) for receiving information from the remote apparatus (10) (page 6, lines 15-16), and processing (24) the information to obtain a usage payment (page 7, lines 16-18); and a local data processing system (11) installed on the remote apparatus (10), having: a monitoring system (14) for gathering usage data from the remote apparatus (10) (page 6, lines 6-7); a processor (processing system 16) for managing the usage data (page 6, lines 10-11); a communications system (20) for communicating information from the processor (16) to the central server (12) (page 6, lines 15-16); and a security system (18), wherein the security system includes an encryption system for securing information transmitted to the central server (page 14, lines 11-16), and for securing information processed by the central server (12) (page 15, line 17 – page 16, line 13).

A forth aspect of the present invention (e.g., claim 33) provides a method for managing usage data collected on a remote apparatus (10), comprising: providing a sensor (14) on the remote apparatus (10) to gather usage data (page 6, lines 6-7); communicating (wireless or wired transmission; page 10, lines 6-17) the usage data to a

processor (16) located on the remote apparatus (10); calculating a charge on the processor (16) based on the usage data (page 6, lines 10-11 and page 6, line 23); and communicating the charge to a server (12) via a wireless transmission channel (page 7, line 10-13; page 6, line 15-16).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-2, 8, 10, 12, 14, and 33 are unpatentable under 35 USC 103(a) over Albertshofer (USPN 6,230,081), hereinafter “Albertshofer,” in view of Van De Pavert (USPN 5,914,471), hereinafter “Van De Pavert.”
2. Whether claims 3-5 and 15 are unpatentable under 35 USC 103(a) over Albertshofer in view of Van De Pavert, further in view of Ando et al. (USPN 5,955,970), hereinafter “Ando.”
3. Whether claim 6 is unpatentable under 35 USC 103(a) over Albertshofer in view of Van De Pavert, in further view of Ando, still in further view of Force et al. (USPN 5,533,123), hereinafter “Force.”
4. Whether claim 9 is unpatentable under 35 USC 103(a) over Albertshofer in view of Van De Pavert, in further view of Ando, still in further view of Force, and still in further view of Davis et al. (USPN 5,844,986), hereinafter “Davis.”

5. Whether claim 10 is unpatentable under 35 USC 103(a) over Albertshofer in view of Van De Pavert, in further view of Dar et al. (US Pub. No. 2001/0039509), hereinafter “Dar.”
6. Whether claim 11 is unpatentable under 35 USC 103(a) over Albertshofer in view of Van De Pavert, still in further view of Ehrman et al. (US Publication 2001/0037298), hereinafter “Ehrman.”
7. Whether claims 16, 21 and 23 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert.
8. Whether claims 17 and 19-20 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, still in further view of Ando.
9. Whether claim 22 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Ando, still in further view of Ehrman.
10. Whether claims 24-25 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, still in further view of Ando, still in further view of Ehrman
11. Whether claims 34-35 and 37-38 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Shimizu et al. (US Publication 2002/0111822), hereinafter “Shimizu.”

12. Whether claim 36 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Shimizu, still in further view of Ehrman.

ARGUMENT

1. Claims 1-2, 8, 10, 12, 14, and 33 are not obvious over Albertshofer in view of Van De Pavert.

Appellants submit that the suggested combinations of the cited prior art do not disclose or suggest each and every claimed feature. For example, with respect to claim 1, Appellants submit that Albertshofer and Van De Pavert do not disclose or suggest, *inter alia*, “a security system including an encryption system for encrypting usage data transmitted between the sensor and the processor.” (Claim 1, parenthetical explanation added). The Office admits this element is not shown in Albertshofer (Final Office Action page 4). Appellants submit that Van De Pavert also does not disclose or suggest, *inter alia*, this feature. In Van De Pavert, the communication of card data is between a card and a secure module 3 of a card operated device 2 (FIG. 2). Neither the card nor the secure module 3 of Van De Pavert gathers usage data from a remote apparatus because neither is a sensor to gather a usage of the telephone, e.g., a timer. The card or the secure module 3 only exchanges data that are already stored in the card. As such, the encryption of Van De Pavert does not disclose or suggest encrypting usage data transmitted between a sensor that gathers usage data and a processor. Thus, the combination of Albertshofer and Van De Pavert could not yield Appellants invention as neither Albertshofer nor Van

De Pavert show this element. This is not, as the Office asserts, arguing the references individually, rather when neither reference shows a claimed element, the combination of references cannot contain that element.

The above arguments also apply to cryptographic circuitry 54 of Van De Pavert (FIG. 4) because the device (card) of FIG. 4 is only an implementation of the FIG. 2 module using “commercially available components,” and cryptographic circuitry 54 does not encrypt usage data transmitted between a sensor that gathers usage data and a processor.

Moreover, in Van De Pavert, block 125 (FIG. 3A) does not encrypt usage data, based on which the processor calculates a charge. Rather, in Van De Pavert, “block 125 executes a pre-defined cryptographic process to encrypt this code and the associated card data on which the code is based[,]” in a verification procedure. (Col. 9, lines 5-7, emphasis added). In Van De Pavert, the card data “includes ... a value of the current card balance[.]” (Col. 8, lines 64-65). However, in the verification procedure of Van De Pavert, a card balance is not a usage data because a use of the card has not taken place. A card balance at this stage may reflect previous usage, but the previous usage will not be used as a basis for calculating a current charge. Actually, Van De Pavert expressly discloses that “this procedure (including encryption) will not take place after each successive adjusting (e.g., reduction) of a card balance.” (Col. 8, lines 5-6, parenthetical explanation added). As such, Van De Pavert does not encrypt a usage data, e.g., time of use because as discussed above, a starting balance of a card in the verification procedure of Van De Pavert does not reflect a usage based on which a charge is calculated. In view of the foregoing, Albertshofer and Van De Pavert, even in suggested combination, do not

disclose or suggest “an encryption system for encrypting usage data transmitted between the sensor and the processor[.]” as claimed in the claimed invention.

With respect to claims 1 and 33, Appellants submit that Albertshofer and Van De Pavert do not disclose or suggest, *inter alia*, “communicating the usage data to a processor located on the remote apparatus; [and] calculating a charge on the processor based on the usage data[.]” (Claim 33, emphasis added; similarly claimed in claim 1). The Office alleges that this feature is taught in paragraph in col. 1, lines 29-39 and the Abstract). However, a careful reading of Albertshofer clearly reveals that the billing data is provided by the base station that is not located on the vehicle (col. 2, lines 19-26). In Albertshofer, the billing system for the vehicle resides at the central unit. In view of the foregoing, Albertshofer fails to teach or suggest a system that calculates a charge on the processor that is “located on the remote apparatus.” Appellants submit that Van De Pavert does not overcome, *inter alia*, this deficiency of Albertshofer. Actually, in the Final Office Action, the Office does not provide a reason/explanation how and why Van De Pavert is used in the rejection of claim 33.

In view of the foregoing, Appellants respectfully submit that claims 1 and 33 are allowable over the art of record.

Claims 2, 8, 10, 12, 14 are allowable for the reasons stated above for claim 1, as well as for their own additional features.

2. Claims 3-5 and 15 are not obvious over Albertshofer, Van De Pavert and Ando.

Appellants submit that Ando does not overcome, *inter alia*, the above-identified deficiencies of Albertshofer and Van De Pavert because Ando does not encrypt usage data transmitted between the sensor that gathers the usage data and the processor. Moreover, Ando fails to show a tamper resistant encasement (claim 3) or a sensor that measures weight placed on a remote apparatus (claim 15). Neither Albertshofer nor Van De Pavert show these elements. Thus, the combination proposed would not yield the invention as defined in claims 3-5 and 15. Claims 3-5 and 15 are allowable for the same reasons stated above for claim 1, as well as for the reasons recited herein.

3. Claim 6 is not obvious over Albertshofer, in view of VanDe Pavert, in view of Ando and further in view of Force.

Appellants submit that Force does not overcome, *inter alia*, the above-identified deficiencies of Albertshofer and Van De Pavert because Force does not encrypt usage data transmitted between the sensor that gathers the usage data and the processor. Moreover, Force fails to show a tamper resistant encasement comprising an epoxy signature embedded therein (claim 6). Force teaches secure digital signatures but never mentions epoxy as part of a tamper resistant encasement. The other references, Albertshofer, Van De Pavert and Ando do not teach this element. Claim 6 is allowable for the same reasons stated above for claim 1, as well as for its own additional features recited herein.

4. Claim 9 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and Ando, Force and Davis do not overcome the deficiencies of Albertshofer and Van De Pavert.
5. Claim 10 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and Dar does not overcome the deficiencies of Albertshofer and Van De Pavert.
6. Claim 11 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and Ehrman does not overcome the deficiencies of Albertshofer and Van De Pavert.
7. Claims 16, 21 and 23 are not obvious over Dar, in view of Van De Pavert.

First it is noted that the Office has provided this rejection (page 10, Final Office Action of April 7, 2008) without discussing Van De Pavert. Instead, the Office appears to be combining Dar with Ando to reject claims 16, 21 and 23. Since Van De Pavert is not mentioned in the rejection, the rejection is defective.

If the Office is combining Ando with Dar, the following argument is submitted. With respect to claims 16 and 23, Dar does not disclose or suggest, *inter alia*, “a local data processing system for gathering data, communicating the usage data to a processor located on the remote apparatus; [and] calculating a charge on the processor based on the usage data[.]” The Office alleges that this feature is taught in paragraph [0039] of Dar in

which billing data is provided. (See Final OA at page 10). However, a careful reading of paragraph [0039] clearly reveals that the billing data is provided by a data processor that is not located on the vehicle, but at a central unit. As detailed, e.g., in paragraph 0157 of Dar, the billing system resides at the central unit. In view of the foregoing, Dar fails to teach or suggest a system that calculates a charge on the processor that is “located on the remote apparatus.” Appellants submit that Ando does not overcome, *inter alia*, this deficiency of Dar. Ando does not encrypt usage data transmitted between the sensor that gathers the usage data and the processor, rather Ando encrypts monetary data used for paying tolls. Appellants submit that claims 16 and 23 are allowable. Dependent claim 21 is also allowable for the reasons stated above.

8. Claims 17 and 19-20 are not obvious over Dar in view of Van De Pavert and further in view of Aldo.

Appellants submit that Ando does not overcome, *inter alia*, the above-identified deficiencies of Dar and Van De Pavert because Van De Pavert is never mentioned in this rejection. Regarding claim 17 Ando fails to show a tamper resistant encasement (claim 17). Neither Dar nor Van De Pavert show this element. Regarding claims 19 and 20, Ando fails to show a central server for receiving the processed usage data. Each of the toll gates of Ando are stand alone systems. Claims 17 and 19-20 are allowable for the reasons recited herein.

9. Claim 22 is allowable for the same reasons stated above for claim 17 and 19-20 above, as well as for its own additional features, and Ehrman does not overcome the deficiencies of Dar, Van De Pavert and Ando.

10. Claims 24-25 are allowable for the same reasons stated above for claim 23, as well as for their own additional features, and Ehrman does not overcome the deficiencies of Dar, Van De Pavert and Ando.

11. Claims 34-35 and 37-38 are not obvious over Dar in view of Van De Pavert, in further view of Shimizu.

Claims 34-35 and 37-38 depend on claim 33 which is allowable in view of Argument 1 which combined Albertshofer and Van De Pavert. In fact Dar is never mentioned in the rejection of base claim 33, so Appellants fail to understand this rejection.

12. Claim 36 is allowable for the same reasons stated above for claims 34-35 and 37-38 (argument 10), as well as for its own additional feature.

In view of the foregoing, Appellants submit that the Office has failed to state a *prima facie* case of obviousness in the final rejection, and the Final Rejection should be reversed.

Respectfully submitted,

/Carl F. Ruoff/

Dated: July 21, 2008

Carl F. Ruoff
Reg. No. 34,241

Hoffman Warnick LLC
75 State Street, 14th Floor
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

CLAIMS APPENDIX

1. A system for processing usage data within a local data processing system installed on a remote apparatus, wherein the local data processing system comprises:
 - a sensor for gathering usage data from the remote apparatus;
 - a processor for processing the gathered usage data and calculating a charge based on the gathered usage data;
 - a security system including an encryption system for encrypting usage data transmitted between the sensor and the processor.
2. The system of claim 1, further comprising a communications system for transmitting the calculated charge to a central server via a wireless transmission channel.
3. The system of claim 2, further comprising a security system, wherein the security system comprises a tamper resistant encasement that encases at least one component of the local data processing system.
4. The system of claim 3, wherein the at least one encased component comprises the processor.
5. The system of claim 3, wherein the at least one encased component comprises the sensor.

6. The system of claim 3, wherein the tamper resistant encasement comprises an epoxy having a signature embedded therein.
8. The system of claim 2, further comprising a security system, wherein the security system comprises an encryption system for encrypting data communicated by the communications system.
9. The system of claim 1, wherein the processor comprises a cryptographic coprocessor.
10. The system of claim 1, wherein the charge comprises an insurance cost.
11. The system of claim 1, wherein the charge comprises a rental cost.
12. The system of claim 1, wherein the remote apparatus is selected from the group consisting of: a vehicle, a boat, an aircraft, a heating system, a home appliance, a medical device, a dwelling, a factory, a commercial establishment, and an insurable object.
13. The system of claim 1, wherein the sensor measures a speed of the apparatus.

14. The system of claim 1, wherein the sensor collects data from a GPS system.
15. The system of claim 1, wherein the sensor measures weight placed on the remote apparatus.
16. A system for managing usage data collected on a remote apparatus, comprising:
a local data processing system having:
a monitoring system for gathering usage data from the remote apparatus;
a processor for processing the usage data;
a communications system for communicating the processed usage data; and
a security system for securing the usage data, wherein the security system includes an encryption system for encrypting usage data communicated from the monitoring system to the processor.
17. The system of claim 16, wherein the security system includes a tamper resistant encasement for securing the processor.
19. The system of claim 16, further comprising a central server for receiving the processed usage data and securing a usage payment, wherein the usage payment is determined from the processed usage data.

20. The system of claim 19, wherein the security system further comprises a second encryption system for encrypting data transmitted between the communications system and the central server.
21. The system of claim 20, wherein the usage payment comprises an insurance payment.
22. The system of claim 20, wherein the usage payment comprises a rental payment.
23. A system for managing usage information collected on a remote apparatus, comprising:
a central server for receiving information from the remote apparatus, and processing the information to obtain a usage payment; and
a local data processing system installed on the remote apparatus, having:
a monitoring system for gathering usage data from the remote apparatus;
a processor for managing the usage data;
a communications system for communicating information from the processor to the central server; and
a security system, wherein the security system includes an encryption system for securing information transmitted to the central server, and for securing information processed by the central server.
24. The system of claim 23, wherein the usage payment comprises an insurance payment.
25. The system of claim 23, wherein the usage payment comprises a rental payment.

33. A method for managing usage data collected on a remote apparatus, comprising:
providing a sensor on the remote apparatus to gather usage data;
communicating the usage data to a processor located on the remote apparatus;
calculating a charge on the processor based on the usage data; and
communicating the charge to a server via a wireless transmission channel.
34. The method of claim 33, further comprising:
obtaining an electronic payment based on the charge.
35. The method of claim 33, wherein the charge is an insurance cost.
36. The method of claim 33, wherein the charge is a rental cost.
37. The method of claim 33, wherein the usage data is encrypted prior to being
communicated to the processor.
38. The method of claim 33, wherein the charge is encrypted prior to being communicated to
the server.

EVIDENCE APPENDIX

There is no evidence submitted.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding.

CERTIFICATE OF SERVICES

There is no other party to this appeal proceeding.